Concept Paper # 255

Name of document to be reviewed: ROI Reallocation

Proposal for reallocation of security gateway and email encryption ROI funds to be utilized for core infrastructure and security architecture upgrades

(Please check one item listed in the following two sections)

Document for review and approval:

__ **Request for Proposal (RFP)**
__ **Request for Service (RFS)**
__ **Request for Quote (RFQ)**
__ **Invitation to Qualify**
__ **Sole Source Procurement**
__ **Statement of Work**
__ **Staff Augmentation**
__ **Master Agreement Purchase**

NOTE: Sole source procurements will also need authorization from DAS Procurement for this type of purchase. Please also contact DAS Procurement at this location: http://das.gse.iowa.gov/procurement/solesource%202010.pdf

Document for review only:

__ **Master Agreement**
__ **Request for Information (RFI)**

Agency:

RFP Reference #: RFB0713005126

Release Date: 3/19/13

This project is requesting IOWAccess funds: Yes ___ No _X__

NOTE: IOWAccess concept papers are to be sent to Wes Hunsberger (Wes.Hunsberger@iowa.gov) for an internal DAS review.

Projected cost over $50,000? Yes _X__ No ___

Projected agency staff hours over 750? Yes ___ No _X__

Project Cost, Funds and Funding Source:

Please list the internal and external resources/costs for the purchase:

Internal Resources/Costs:

Costs

Equipment	$259,904
Contingency	$15,000.00
Manpower	100 hours FTE time
Total	$274,904

Funds to be reallocated from project L103, FY 12
"Security Gateway and Enterprise E-mail Services"

Allocated	$300,000
Spent	$0.00
Balance	$300,000

External Resources/Costs:

Timelines:

Estimated

Acquire equipment:	April 2013
Installation:	May, 2013
Begin production, complete project	1 Sept. 2013

Goal:

Provide monitor and test points in the new ITE core network for both ITE Network Team and DAS/ISO Security Office.

Background:

The computer data network designed and operated by DAS/ITE is used by almost every State of Iowa executive branch agency. This network is commonly referred to as the campus network, although physical and logical parts of the network exist as far away as Johnston.

In the past 15 years the campus network has grown from a simple federation of agency-owned Token Ring nodes used primarily to access main frame services to an Ethernet core network that provides connections to a plethora of hosted common services such as I3, Web Warrants, E-mail, and Enterprise A&A. In addition, the core network is now used by most agencies to connect their employees to the Internet and for State of Iowa customers worldwide to connect to Iowa.

The core network is now being upgraded and expanded once again. The entire core of the network in the Hoover building, access point for many of the agencies resources, is being modernized to the next generation of equipment, not only in terms of more efficiency but especially in terms of expandability and

raw speed. All of this activity fuels the move towards a consolidated, highly collapsed architecture as agencies abandon their legacy networks.

The need to secure and maintain a highly available, highly secure environment increasingly falls to DAS/ITE and DAS/ISO as agencies unencumber themselves from making data flow to making their business charter their top priority. These tasks have always been daunting but now take on the added challenge of increasing in scale at a time when network equipment is less oriented and, therefore, less equipped to provide monitoring facilities.

Two DAS entities must have access to data as it flows into, through and out of executive branch agencies; DAS Security Office (ISO) and DAS/ITE Networking

ISO must have access to detect malware, record access, and guard against data loss to malevolent outsiders. Networking must be able to access data to troubleshoot problems that arise do to defective equipment or to ensure enough network space is available to the applications that agencies and State of Iowa patrons use.

The always-expanding need to collect, detect, measure and fix data concerns has led to contention for access to network ports that are placed in the right locations, on equipment that has a minimal number of connections for this purpose. ISO generally has first access too hard to get at ports. When Networking needs to troubleshoot a problem ISO's equipment must be disconnected for the duration of Networking's investigations, leaving a hole in the daily record of data ISO must accumulate. Many of these changes to who gets the data require changes to the configuration of the network equipment itself; equipment carrying production information. While these changes are generally harmless there is always a things could go awry.

ISO must deploy many instances of detection devices to keep up with all of the places they should or are requested to monitor. In some cases, these devices are underutilized, leading to an inefficient use of people and material. In other cases monitoring equipment cannot keep up with the data flow, leading to dropped or lost monitoring periods.

In the same way that ISO has issues with acquiring data the Networking team does as well. Networking's predicament is that troubleshooting is rarely deterministic. Having data collection points that don't eventually conflict with ISO is a luxury.

With so many activities contending for data the problems worsens with the installation of a new network core. Network equipment is designed to move data. Monitoring the data flows is often a second thought. In fact, changes to equipment configuration have led to a reduction of available ports to use for distribution to collection tools. In some cases, network equipment that is past its supportable use date is still on the job, being used as access points to get at the required data flow and get it to the number of tools required.

What is needed is a way to upgrade the ability of ISO and Networking to simultaneously monitor data interfaces at new, higher speeds, with equipment designed to handle the throughput. All of this without requiring one entity to disconnect for the other to do their job, or reconfigure the network device during prime operating hours.

What is needed is an upgrade to the way data is captured and dispensed in this growing, high-speed core network.

Expected Results:

What are the tangible and intangible benefits of this purchase for this agency and/or state government?

Purchase of this equipment will allow for the creation of a core data monitoring fabric parallel to the new core network. This concept and practice is already in use in State of Iowa government at the University of Iowa hospitals, at Iowa State University and at the ICN.

The fabric will use the monitoring facilities available in the network equipment but will also include purpose-built taps that capture all of the flowing from place to place and require no disruption of the production data network to use.

By bringing this data into the monitoring fabric data from a single tap can be sent to multiple tools at the same time. This one-to-many capability can allow ISO and Networking to be monitoring the same data flows but with different tools and for different purposes. This non-disruptive quality brings ISO closer to the time when 100% of the data they seek will be acted upon. It also allows Networking to have multiple views of the same data, so that a tool recording bandwidth doesn't need to be taken off line to allow staff to diagnose problems.

By the same token, the monitoring fabric will be used to concatenate many lower-speed connection points to a single collection tool, minimizing the waste of equipment it would take to deploy and maintain individual tools.

This same fabric will be used to load balance important high-speed flows across an array or cluster of the same tool, such as an Intrusion Detection device. By building this array and load balancing the output of the fabric sending data to the array, any single given element of the array can be taken off-line form maintenance, etc. without jeopardizing the collection of data.

The controllers of the network fabric also allow data to be filtered so that only flows of interest are captured. This allows for the elimination of wasted cycles and space to record nightly reoccurring backup data or network chatter that each of the network switches use to communicate with each other.

In the future, equipment purchased here can be expanded to the Lucas building, where it's collection points can be joined to the data in the Hoover building to further provide economies of scale, not only in terms of less equipment as compared to individual devices, but also in terms of the need to have a corresponding number of man-hours to maintain individual devices.

Can these benefits be quantified in financial terms? If yes, please explain.

Yes. Faster troubleshooting, resulting in less downtime when outages occur.

How will you be more effective as a result of this purchase?

Collection tools will not need to be swapped in and out to view data or make decision about security issues.

How will service to your customers be enhanced as a result of this purchase?

Faster and more complete service results in less downtime and more agency productivity.

Testing and Acceptance:

As new network core equipment is added to test and then production the monitoring fabric will be deployed alongside it. Acceptance testing includes attaching existing tools and comparing outputs to other tools still in use on other parts of the network.

Some of the Interested Parties:

DAS/ITE Networking
DAS/ISO

Some of the Recipients of this Service:

Every State of Iowa executive branch agency or board

Standards:

Solution will meet all security standards

Architecture:

Solution meets architecture requirements and improves the overall networking and security posture for the state.

Business Continuity / Disaster Recovery:

Solution will improve Business Continuity and Disaster Recovery capabilities.

Recommendations from the State CIO:

NOTE: *Where applicable, all DAS GSE Procurement and IA Administrative Code 11-105 and 11-106 requirements and procedures are to be followed. Reference: http://das.gse.iowa.gov/procurement/, specifically: http://das.gse.iowa.gov/procurement/adminrules/.*

Duplication recommendation from the State CIO to the DAS Director:

a) Is there duplication within Government? *(Please identify duplication at the agency level, as well as within the enterprise)*
b) Can an existing program be modified to address a new need?
c) Do you have any similar program in existence?
d) Have you sought IT procurements for similar programs in the past?
e) Do you have purchasing documents for similar programs?
f) Do you have similar purchasing documents that could be used as a starting point for this program?
g) Is there anything you could provide that could assist the agency with this IT procurement?
h) Are there alternatives available to the agencies?

Recommendation of the State CIO to the DAS Director:

Authorize this IT procurement Yes _X_ No ___
Alternatives suggested by the State CIO (see comments below) Yes ___ No _X_

Additional comments from the State CIO:

Recommendation is for approval by the TEC and was subsequently was approved by the State CIO.

DAS Director's action:
Authorize this IT procurement Yes _X_ No ___

DAS Director's signature and date:

The above IT procurement concept approved by Director Carroll on __5/1/13__

Comments: **None.**